RESEARCH-ARTICLE

Towards Understanding User Privacy Concerns of Internet of Things Sensor Data

DIPU RAM ROY, Bangladesh University of Engineering and Technology, Dhaka, Dhaka, Bangladesh

JIEQIONG ZHAO, Augusta University, Augusta, GA, United States

SHIJIA PAN, UC Merced, Merced, CA, United States

SHIWEI FANG, Augusta University, Augusta, GA, United States

Published: 06 May 2025

SenSys '25: The 23rd ACM Conference on Embedded Networked Sensor Systems
May 6 - 9, 2025
CA, Irvine, USA

Conference Sponsors:
SIGBED
SIGOPS
SIGMOBILE
SIGARCH
SIGMETRICS

Sensors S&P '25: Proceedings of the 2nd International Workshop on Security and Privacy of Sensing Systems (May 2025)
https://doi.org/10.1145/3722566.3727627
ISBN: 9798400716126

Towards Understanding User Privacy Concerns of Internet of Things Sensor Data

Dipu Ram Roy
rdipu.roy01@gmail.com
BUET
Dhaka, Bangladesh

Jieqiong Zhao
jiezhao@augusta.edu
Augusta University
Augusta, GA, USA

Shijia Pan
span24@ucmerced.edu
Univ. of California, Merced
Merced, CA, USA

Shiwei Fang
shfang@augusta.edu
Augusta University
Augusta, GA, USA

ABSTRACT

Despite the wide adoption of Internet of Things (IoT) devices in people's lives, their privacy implications remain unclear to many users. Privacy policies are used as the major mechanism to deliver this information, and tools are developed to assist users to interpret these policies, there is still a gap between users' perceived privacy and the actual privacy risks they face. Especially for various indirect sensing modalities, where users' comprehension and concerns about their privacy are unknown. We present *PrivacyVis*, a novel visualization tool that provide an informative and expressive visual representation of the sensors, data processing workflows, and associated privacy risks of IoT devices. Designed to be user-friendly, the tool aims to enhance users' understanding and empower them to make informed decisions about their privacy. *PrivacyVis* allows us to conduct efficient user surveys to understand user concerns and perceived privacy for IoT devices.

ACM Reference Format:
Dipu Ram Roy, Jieqiong Zhao, Shijia Pan, and Shiwei Fang. 2025. Towards Understanding User Privacy Concerns of Internet of Things Sensor Data. In *Proceedings of Sensors S&P (SensorsSP'25)*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3722566.3727627

1 INTRODUCTION

The growth of the Internet of Things (IoT) sensing systems introduces many new sensing modalities and enables many intelligent services, such as smart home control, health care, and security systems. These human-centric systems use various sensors to capture human information to achieve the designated functionalities. Sensors such as cameras and microphones capture signals that users can easily understand, while sensors such as WiFi [1, 6, 7], mmWave [8, 11], light [16], vibration [13, 20], ultrasound [3], and thermal [2], are used to capture indirect signals of human presence in the environment for non-intrusive monitoring with privacy consideration. When these sensors become increasingly integrated into ambient environments, users are often unaware of their privacy implications due to the lack of understanding of their working principles.

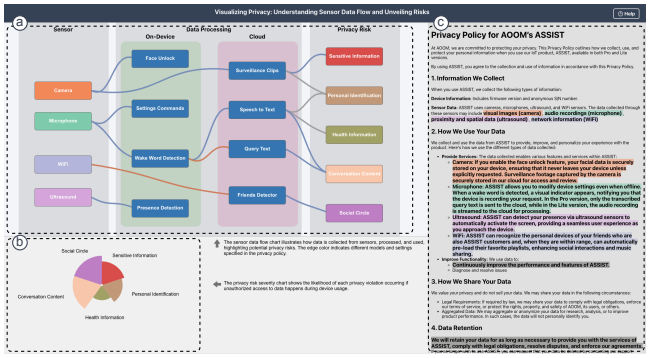

Figure 1: *PrivacyVis* Website. The visualization tool comprises three coordinated panels: ⓐ a Sensing Privacy Risk Pathway panel (Sankey Diagram). It maps the data flow from sensors through processing stages to associated privacy risks. ⓑ a Privacy Risk Severity panel (Radial Bar Chart). It quantifies privacy risks by exposure likelihood. and ⓒ a Privacy Policy panel (Text). It presents the privacy policy with highlighted text for specific sensors and privacy risk categories.

Privacy policies from manufacturers are the primary means for users to understand a device's privacy implications. However, these policies are often lengthy and have an emphasis on legal perspectives, which makes it difficult for users to interpret the device's capability related to privacy implications. As a result, users may struggle to comprehend the extent to which their personal data is **collected, processed, and shared**. Furthermore, many IoT devices continuously collect and process the sensor data. However, there is often a lack of transparency regarding how the data is processed. The challenge of comprehending privacy policies and the lack of operational transparency contribute to the information asymmetry between users and service providers, exacerbating the privacy knowledge gap. This knowledge gap prevents users from making informed decisions about the privacy risks of IoT devices.

Privacy policy comprehension tools are designed to assist users with their understanding of where their data is stored and processed, as well as which third parties might receive it [12]. However, users without domain knowledge often find it difficult to associate this information with the impact on their daily lives beyond the basic functionalities of the device – there is a gap between users' perceived privacy and the risks conveyed by these policies. Especially when manufacturers utilize "dark patterns", which are deceptive user interfaces [18]. For example, some modern vehicles with internet capability offer features that help drivers monitor their driving behaviors with the potential to improve them. Yet, their privacy policies fail to clarify that by sharing this data with data brokers,

Sensors S&P '25, May 6-9, 2025, Irvine, CA, USA

ACM ISBN 979-8-4007-1612-6/2025/05
https://doi.org/10.1145/3722566.3727627

who may share it with insurance companies, drivers' insurance premiums may increase [25]. In this case, the disconnection between the privacy risks users perceive (how often and where they drive) and the potential impact (an increase in insurance premiums) results in the information gap.

With ongoing developments in sensors and algorithms, seemingly irrelevant data can provide valuable insights that have significant impacts on various aspects of users' lives. These impacts could range from higher insurance premiums for auto, home, and health coverage, to identity theft and scams. However, it's still unclear how much users care about these potential risks, especially those with a lower probability of occurring. Additionally, personal privacy preferences are not static; they evolve over time as technology advances and contexts change [14, 27].

Another challenge in helping users understand privacy implications is that individuals typically fall into three categories: 15%-25% are fundamentalists, who are highly concerned about privacy and distrust various entities; 15%-25% are unconcerned, trusting existing frameworks; and 40%-60% are pragmatists, who acknowledge risks but tend to trust [14, 26]. With preconceived notions of privacy and an ever-increasing flow of information coupled with shortened attention spans [17, 19], effectively communicating the increasingly complex implications of privacy risks is a growing challenge.

To assess how technology can assist users in understanding privacy implications and gauge their concerns about privacy, we propose a user survey through the development of an interactive web-based visualization tool – *PrivacyVis* [23], as shown in Figure 1 – designed to enhance user comprehension of IoT device privacy risks. *PrivacyVis* provides an informative and expressive representation of the sensors involved in data collection, the subsequent processing steps, and the potential privacy risks associated with the use of these devices. With a straightforward, accessible interface, we envision *PrivacyVis* as a tool that empowers users to better understand how their data is used and the privacy risks they might face. Our goal is to bridge the information gap and help users navigate the complex privacy landscape of modern IoT technologies.

2 RELATED WORK

Prior research has highlighted the increasing importance of usable privacy in research [22], as well as how Privacy-Enhancing Technologies (PETs) can enforce legal privacy principles [9]. While some PETs, such as the Tor network [4], are effective in minimizing privacy-related data, they are less efficient when dealing with data from IoT sensors. PETs for IoT devices tend to function more as Transparency-Enhancing Tools (TETs) [10], which inform users about how their data is processed. These tools are designed to address the situation where most people do not read privacy policies [24]. Early works, such as Privacy Nutrition Labels [15], explored the use of labels to summarize privacy policies, while annotated text has been used to help users more easily find specific information within privacy policies [28]. Poli-see [12] has also explored the use of visualization to inform users about data flow and usage. More recent studies have focused on IoT devices: Emami-Naeini et al.[5] investigated what should be included in privacy and security labels for IoT devices, while OnLITE[21] developed an online tool to help non-expert consumers visualize how IoT devices handle data. In contrast to efforts focused on summarizing or visualizing privacy policies, PrivaSee [29] explored how Augmented Reality (AR) can be used to inform users about sensor range in physical space. While these works have advanced the communication and education of non-expert users regarding privacy concerns related to their devices, they fall short of bridging the gap between user perceived privacy, sensor data, and the potential impact on their lives.

3 SYSTEM DESIGN

3.1 Privacy Policy Visualization

PrivacyVis [23] is designed to enhance user understanding of IoT sensor data's privacy risks through three coordinated panels: (1) a **Sensing Privacy Risk Pathway panel** in the form of Sankey Diagram (Figure 1 ⓐ), illustrating the data flow from sensors to data processing and their associated privacy risks; (2) a **Privacy Risk Severity panel** in the form of Radial Bar Chart (Figure 1 ⓑ), demonstrating the likelihood of privacy exposure; and (3) a **Privacy Policy Text panel** (Figure 1 ⓒ) that displays privacy policies associated with the IoT sensors, with color-coded content [28] corresponding to specific sensors and data processing. The brushing and linking interaction among these three coordinated panels is shown in Figure 2. Panels (a.1), (b.1), and (c.1) display the website in its initial state, while panels (a.2), (b.2), and (c.2) show the updates after one of the nodes (e.g., Microphone) in the Sensing Privacy Risk Pathway panel is clicked.

The **Sensing Privacy Risk Pathway panel** aims to mitigate the gap between user-perceived privacy and the risks conveyed by these policies. The **Sensor** component covers a wide range of sensors used for human sensing, including direct sensing modalities, such as camera and microphone, and indirect sensing modalities, such as WiFi, mmWave, vibration, light, etc. The **Data Processing** component illustrates tasks performed on the data collected by these sensors, such as "face unlock" and "wake word detection." These tasks are organized based on their processing location, **On-Device** versus **Cloud**-based processing, and this distinction is increasingly important as their risk levels vary. We employ color encoding to convey this risk level difference. The **Privacy Risk** component provides concrete examples of privacy risks and depicts its association with the corresponding processing. For example, users may be aware that recordings of conversations can expose content but may not realize that these recordings could also be used for health assessments. When users explore the panel, the connected paths and nodes will be highlighted when the mouse hovers over a node, as shown in Figure 2 (a.2). Clicking on a node keeps the highlight active and triggers the linking interaction across the other panels. Panel (a.2) also shows all possible privacy risks associated with the selected sensor. By visualizing these connections, users can better recognize the privacy implications of their data.

The **Privacy Risk Severity panel** depicts the assessment of the likelihood of privacy leakage. While data extraction and associated privacy leakage may be possible in some cases, the likelihood of such occurrences can vary. This panel enables users to assess the potential risk of privacy breaches related to their information. The radius of each privacy risk radial bar corresponds to the assessed

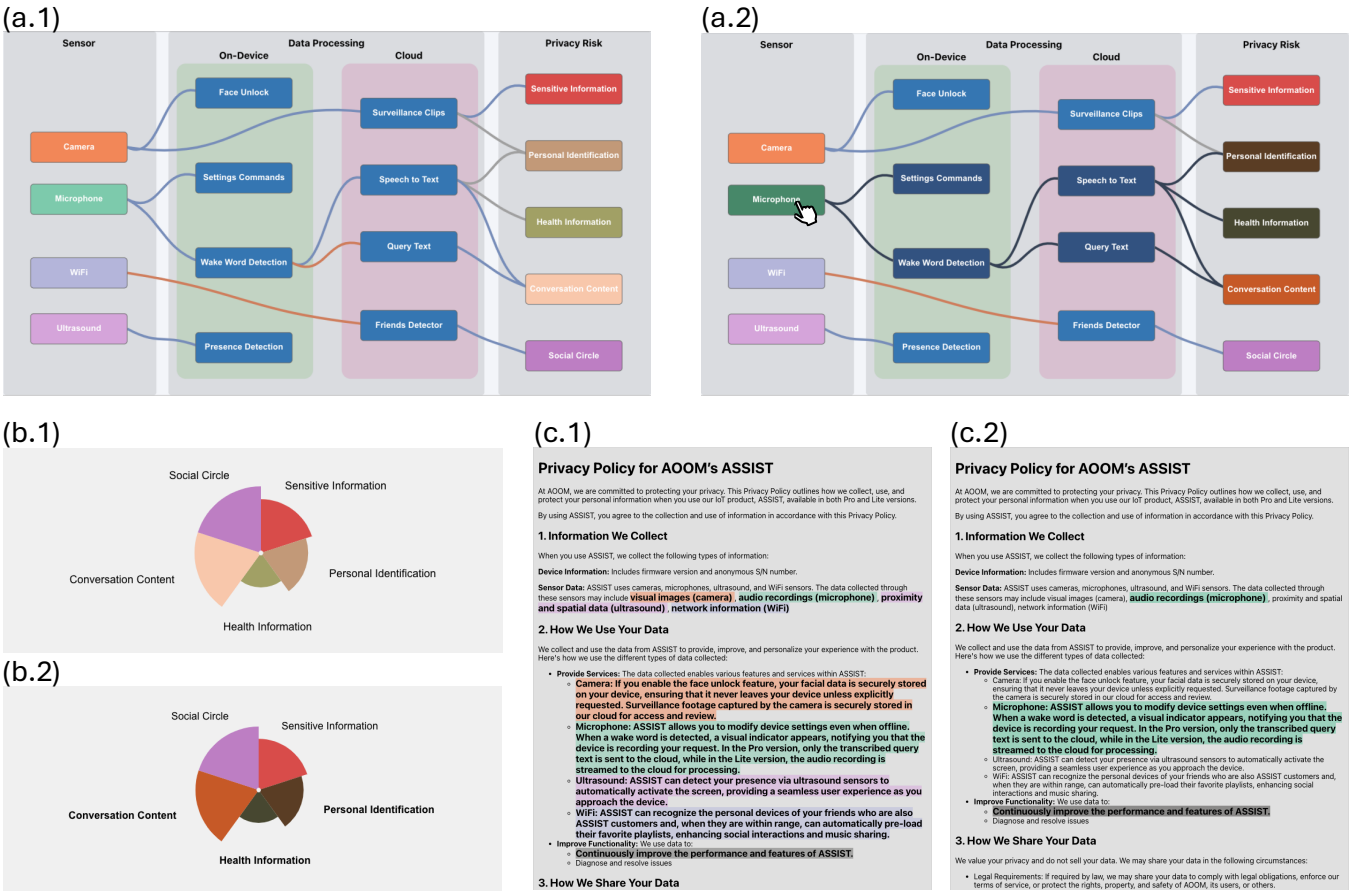

Figure 2: *PrivacyVis* interaction. The main interactive feature on this website is the Sankey Diagram, which initiates brushing and linking. When a user hovers over a node, the connected nodes will be highlighted. If the user clicks on a node, the Sankey Diagram will transition from (a.1) to (a.2), and the relevant privacy policy will be highlighted as shown in (c.2). Meanwhile, the Radial Bar Chart will update from (b.1) to (b.2).

risk level, with a larger radius representing higher risks. For example, the leakage of audio recordings will reveal "conversation content", while such recordings might only expose "health information" if the user has health concerns affecting their speech. The difference in the risk severity is shown in the Figure 1 ⓑ where "conversation content" has a larger radius than "health information." When a node in the Sankey Diagram is clicked, the corresponding radial bars are highlighted, as shown in Figure 2 (b.1) and (b.2). Additionally, hovering over a bar triggers a tooltip displaying the assessed risk severity level.

The **Privacy Policy Text panel** displays the highlighted privacy policy text for the IoT device. The background color of the highlighted text corresponds to the **Sensor** component in the **Sensing Privacy Risk Pathway panel**, enabling users to quickly identify which parts of the policy relate to specific sensors when exploring privacy risks. This color encoding also facilitates the comparison of how a single privacy policy – cover different models of an IoT devices family (e.g., lite vs. premium versions) – may affect where data is processed for each model. Additionally, the panel highlights sections of text where no specific sensor is mentioned. For example, a privacy policy statement such as "continuously improve the performance and features" could apply to any sensor data. Such general statements may indicate potential feature developments that introduce new privacy risks, which may not align with user expectations. Examples of the highlighted privacy policy text are shown in Figure 2 (c.1) and (c.2). Panel (c.1) represents the initial state, where all relevant privacy policy text is highlighted with background colors corresponding to different sensors. Panel (c.2) shows the updated view after a sensor is selected in the **Sensing Privacy Risk Pathway panel**. In this updated state, general statements remain highlighted in gray to indicate potential risks affecting non-specific sensors, while background highlights for other sensors are removed to focus the user's attention on the text related to the selected sensor.

3.2 User Study

To evaluate the effectiveness of *PrivacyVis* in enhancing people's understanding of privacy risks regarding the hypothetical IoT device, we plan to conduct a 30-minute online user study with public

audiences. The goal of the study is to assess how well the tool helps people comprehend the nuanced relationships among privacy policies, sensor data, and associated risks, as well as to increase people's awareness of potential privacy risks of IoT devices. We will recruit online participants using a variety of methods, including targeted bulletin board posts for students, faculty, and staff at multiple institutes, as well as outreach through online forums related to IoT devices and privacy.

Our study consists of three key phases. In the pre-task survey, participants complete a short questionnaire to provide background information on their experiences with IoT privacy policies. Next, in the exploratory analysis of the *PrivacyVis* website, participants freely explore the site, with a few initial questions to facilitate engagement. Finally, in the post-task survey, participants provide feedback on their experience and reflect on what they learned.

In both the pre-task and post-task surveys, participants rate their agreement with IoT privacy-related statements on a 5-point Likert scale. Example statements include: their willingness to pay more for an IoT device if data were processed locally rather than sent to online servers, their perception of IoT devices' effectiveness in protecting personal data, and whether they feel forced to choose between privacy loss and functionality. Comparing pre-task and post-task ratings will reveal changes in participants' understanding of privacy risks and shifts in their attitudes.

To encourage deeper reflection, the post-task survey also includes open-ended questions, such as whether engaging with *PrivacyVis* increased their confidence in understanding privacy policies and data handling practices. These qualitative responses will help uncover nuanced shifts in participants' perspectives on IoT privacy.

4 DISCUSSION

This work is still a work in progress, and as such, we are unsure how users will react to the visualization tool or how concerned they will be about IoT sensing privacy risks. However, it is important to discuss some of the design choices and potential gaps in the tool. Unlike prior works, this visualization tool incorporates additional information not typically found in privacy policies, such as the "privacy risk" indicators in the **Sensing Privacy Risk Pathway panel** and the **Privacy Risk Severity panel**. These risks represent potential information associated with the user that could be leaked, with the likelihood of such leaks displayed in the **Privacy Risk Severity panel**.

We have included these risks to bridge the gap between users' perceived privacy concerns and the actual sensor data. The inclusion of these risks serves as clear examples intended to help users calibrate their preconceived notions. However, the tool still lacks coverage of the full range of potential impacts that evolving sensors and algorithms may have on users' daily lives. This is particularly relevant in the context of side-channel attacks, which can present severe privacy risks.

It is impossible to list all potential risks, as some attacks or how certain companies may use the data are not publicly known. Additionally, listing every possible risk could overwhelm users with information, which would be counterproductive given their limited attention span and domain knowledge. Therefore, more careful research is needed to determine how to effectively guide users without overwhelming them or relying on hearsay.

5 CONCLUSION AND FUTURE WORK

We discuss how our proposed visualization tool, *PrivacyVis*, can help bridge the gap between users' perceived privacy concerns and the actual information revealed by sensors in IoT devices. By incorporating potential privacy risks associated with sensor data, we aim to guide users in adjusting their perceptions to better align with these risks.

We plan to fine-tune *PrivacyVis* to make it more effective and suitable for a broad range of users. Additionally, we outline the steps for our user study, which we intend to conduct rigorously to explore the extent of users' concerns about their privacy. With user feedback, we aim to further refine the design of our privacy visualization tool to improve its usability for non-expert users.

REFERENCES

[1] Fadel Adib and Dina Katabi. 2013. See through walls with WiFi!. In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*. 75–86.

[2] Alex Beltran, Varick L Erickson, and Alberto E Cerpa. 2013. Thermosense: Occupancy thermal based sensing for hvac control. In *Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings*. 1–8.

[3] Roland Cheng, Wendi Heinzelman, Melissa Sturge-Apple, and Zeljko Ignjatovic. 2011. A motion-tracking ultrasonic sensor array for behavioral monitoring. *IEEE sensors journal* 12, 3 (2011), 707–712.

[4] Roger Dingledine, Nick Mathewson, Paul F Syverson, et al. 2004. Tor: The second-generation onion router.. In *USENIX security symposium*, Vol. 4. 303–320.

[5] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.

[6] Shiwei Fang, Ron Alterovitz, and Shahriar Nirjon. 2019. Non-line-of-sight around the corner human presence detection using commodity wifi devices. In *Proceedings of the 1st ACM International Workshop on Device-Free Human Sensing*. 22–26.

[7] Shiwei Fang, Tamzeed Islam, Sirajum Munir, and Shahriar Nirjon. 2020. Eyefi: Fast human identification through vision and wifi-based trajectory matching. In *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 59–68.

[8] Shiwei Fang and Shahriar Nirjon. 2020. Superrf: Enhanced 3d rf representation using stationary low-cost mmwave radar. In *International Conference on Embedded Wireless Systems and Networks (EWSN)...*, Vol. 2020. 120.

[9] Simone Fischer-Hübner. 2009. *Privacy-Enhancing Technologies*. Springer US, Boston, MA, 2142–2147. https://doi.org/10.1007/978-0-387-39940-9_271

[10] Simone Fischer-Hübner and Farzaneh Karegar. 2024. *The Curious Case of Usable Privacy: Challenges, Solutions, and Prospects*. Springer.

[11] Tianbo Gu, Zheng Fang, Zhicheng Yang, Pengfei Hu, and Prasant Mohapatra. 2019. Mmsense: Multi-person detection and identification via mmwave sensing. In *Proceedings of the 3rd ACM Workshop on Millimeter-wave Networks and Sensing Systems*. 45–50.

[12] Wentao Guo, Jay Rodolitz, and Eleanor Birrell. 2020. Poli-see: An interactive tool for visualizing privacy policies. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES'20)*. ACM, New York, 57–71. https://doi.org/10.1145/3411497.3420221

[13] Zhizhang Hu, Yue Zhang, Tong Yu, and Shijia Pan. 2022. VMA: Domain variance- and modality-aware model transfer for fine-grained occupant activity recognition. In *2022 21st ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 259–270.

[14] Giovanni Iachello, Jason Hong, et al. 2007. End-user privacy in human–computer interaction. *Foundations and Trends® in Human–Computer Interaction* 1, 1 (2007), 1–137.

[15] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, Article 4, 12 pages.

[16] Tianxing Li, Chuankai An, Zhao Tian, Andrew T Campbell, and Xia Zhou. 2015. Human sensing using visible light communication. In *Proceedings of the 21st annual international conference on mobile computing and networking*. 331–344.

[17] Philipp Lorenz-Spreen, Bjarke Mørch Mønsted, Philipp Hövel, and Sune Lehmann. 2019. Accelerating dynamics of collective attention. *Nature communications* 10, 1 (2019), 1759.

[18] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a light on dark patterns. *Journal of Legal Analysis* 13, 1 (2021), 43–109.
[19] Gloria Mark. 2023. *Attention span: A groundbreaking way to restore balance, happiness and productivity.* Harlequin.
[20] Shijia Pan, Mostafa Mirshekari, Jonathon Fagert, Ceferino Gabriel Ramirez, Albert Jin Chung, Chih Chi Hu, John Paul Shen, Pei Zhang, and Hae Young Noh. 2018. Characterizing human activity induced impulse and slip-pulse excitations through structural vibration. *Journal of Sound and Vibration* 414 (2018), 61–80.
[21] Alexandr Railean and Delphine Reinhardt. 2021. OnLITE: on-line label for IoT transparency enhancement. In *Secure IT Systems: 25th Nordic Conference, NordSec 2020, Virtual Event, November 23–24, 2020, Proceedings 25.* Springer, 229–245.
[22] Christian Reuter, Luigi Lo Iacono, and Alexander Benlian. 2022. A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead. , 2035–2048 pages.
[23] Dipu Ram Roy, Jieqiong Zhao, Shijia Pan, and Shiwei Fang. 2025. Poster Abstract: PrivacyVis: Interactive Visualization Tool for Privacy Risks of Internet of Things Sensors. In *Proceedings of the 23nd ACM Conference on Embedded Networked Sensor Systems.*
[24] H Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35, 4 (2011), 989–1015.
[25] The New York Times. 2024. Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies. https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html. Accessed: Mar. 9, 2025.
[26] A Westin. 2001. Opinion surveys: What consumers have to say about information privacy, SoC: The House Committee on Energy and Commerce, Trade, and Consumer Protection.
[27] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.
[28] Shomir Wilson, Florian Schaub, Frederick Liu, Kanthashree Mysore Sathyendra, Daniel Smullen, Sebastian Zimmeck, Rohan Ramanath, Peter Story, Fei Liu, Norman Sadeh, and Noah A. Smith. 2018. Analyzing privacy policies at scale: From crowdsourcing to automated annotations. *ACM Transactions on the Web* 13, 1, Article 1 (2018), 29 pages.
[29] Yue Zhang, Shangjie Du, Jiqing Wen, Robert Likamwa, Shiwei Fang, and Shijia Pan. 2024. Poster: PrivaSee: Augmented Reality-Enabled Privacy Perception Visualization for Internet of Things. In *Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services.* 694–695.